

如何删除（停用）系统或浏览器中的 CNNIC 证书

V 1.32

一、为什么要删除（停用）系统或浏览器中的CNNIC证书（CNNIC根级证书的危害性）	2
二、如何删除Windows XP系统中的CNNIC证书（适用于IE、Chrome等浏览器）	2
1、导入CNNIC证书到证书管理器中的信任区域	2
2、在证书管理器受信任的根证书颁发机构栏目中停用CNNIC证书.....	4
3、再次导入CNNIC证书并到证书管理器中的不信任的证书区域.....	7
4、特别说明.....	8
三、如何停用Firefox 3.6 中的CNNIC证书.....	9
1、导入证书.....	9
2、禁用证书.....	11
3、特别说明(必读).....	13
四、如何在Opera浏览器中停用CNNIC证书.....	14
特别说明.....	16
五、屏蔽Mac的Safari浏览器CNNIC证书.....	17
六、关于部份银行网站使用CNNIC签名问题	17
七、关于停用CNNIC证书的相关操作的重要说明（必读）	18
1、关于CNNIC五个相关证书名称的问题	18
2、关于系统与浏览器在线更新后CNNIC证书停用状态是否会改变的问题.....	18
3、关于系统不同登录用户CNNIC证书停用状态的问题.....	18
八、技术支持.....	18

一、为什么要删除（停用）系统或浏览器中的 CNNIC 证书（CNNIC 根级证书的危害性）

中共控制的 CNNIC 在中国网民中被称为最大的流氓网络信息管理与服务机构。微软与 Firefox 等浏览器在根证书列表里已将 CNNIC 列为“受信任的根证书发行机构”。这样，访问由 CNNIC 颁发证书的 https 协议网站将不会被用户觉察到有任何警告，而以前你的浏览器访问这类网站会跳出严重警告。因为中共控制了国内域名服务，国内某些被监控的用户访问海外网站，比如海外邮箱时，可能被转向到 CNNIC 设置的代理服务器。这样的代理服务器可以用自己伪造的海外邮箱安全证书终结用户的 https 安全链接而窃取个人信息，同时代替用户连结海外邮箱。因现在 CNNIC 伪造的安全证书是微软与 Firefox 等浏览器等信任的，所以用户将毫无察觉，还以为自己是安全链接到海外邮箱的呢。国外用户也可能因“中间人攻击”而同样受害。比如无线上网用户可能误用了附近的恶意无线热点，或自己上网线路被转接等。以前即使这些发生，只要一上 https 网站浏览器就会严重警告说安全证书是伪造的，现在就没有这种警告了。这就使得 https 协议的安全证书完全失去了安全访问的意义，也就是说以前中共做不到的攻击现在可以成为现实了。鉴于此，为上网的安全考虑，建议国内和国外用户删除（停用）CNNIC 证书。

二、如何删除 Windows XP 系统中的 CNNIC 证书（适用于 IE、Chrome 等浏览器）

此方法适用于采用微软 CA 目录的浏览器，如：IE、Chrome、Safari、Dragon、Myie 等浏览器。

步骤：

1、 导入 CNNIC 证书到证书管理器中的信任区域

（注：先加入到信任区，然后停用，防止系统更新时检测到没有此证书而直接添加且激活为证书启用状态，也为后面将其纳入不信任证书做准备）

将下载的证书文件解压后，得到五个证书文件，即：

CNNIC Root.cer （序列号 49 33 00 01）

CNNIC_SSL.cer （序列号 49 33 00 15）

CNNIC_SSL_After_2010.03.01.cer （序列号 42 87 a2 a0）

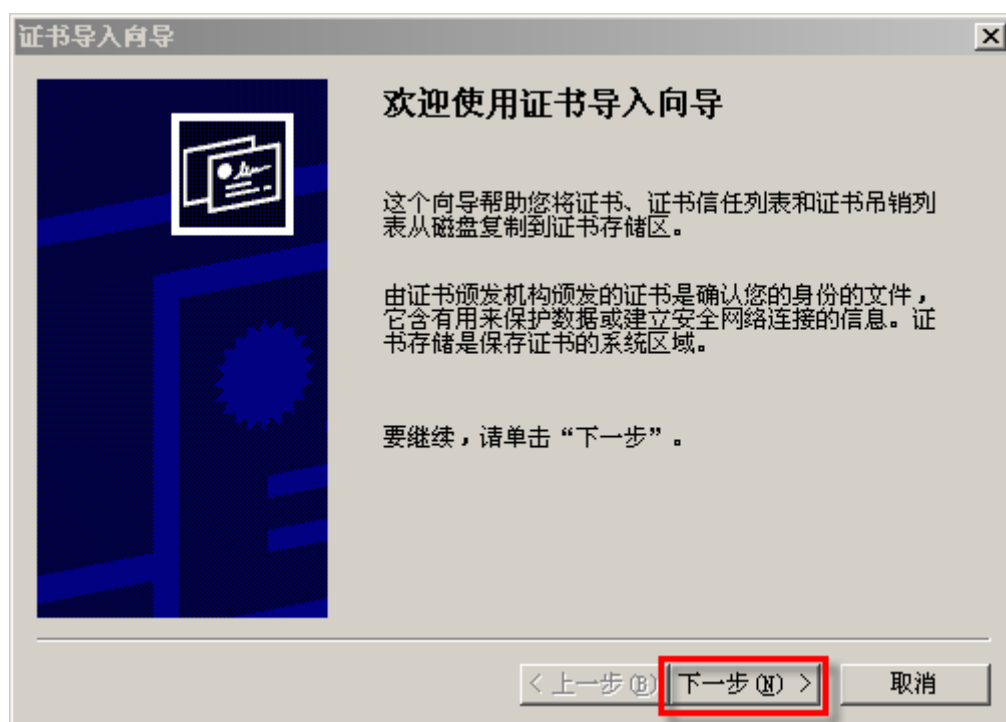
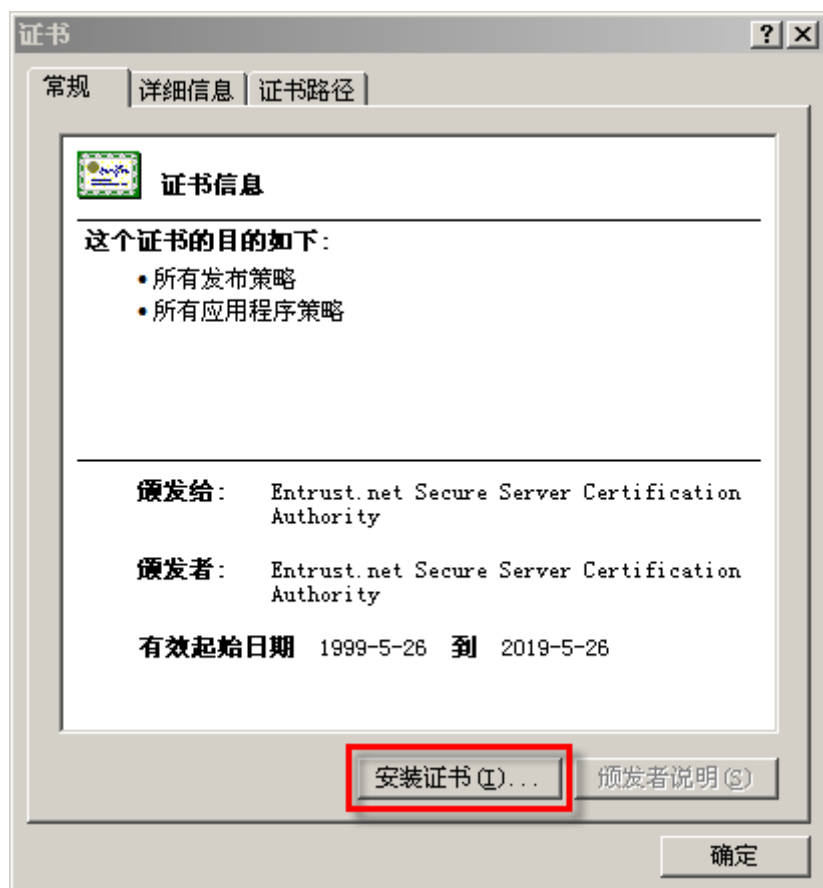
CNNIC_SSL_Before_2010.03.01.cer （序列号 49 33 00 29）

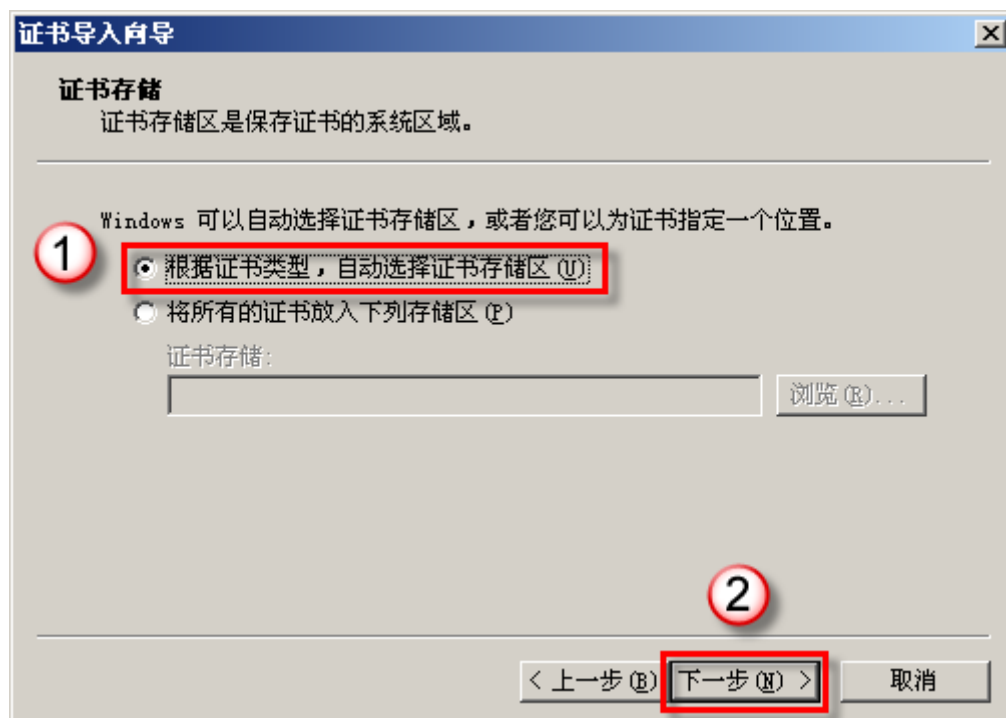
Entrust.net Secure Server Certification Authority.cer （序列号 37 4a d2 43）

分别双击这五个证书文件按提示安装，在安装过程中，一直选中默认的设置，方法如下：

双击以上各文件→安装证书→下一步→选择“根据证书类型，自动选择证书存储区”→下一步→完成→确定→确定。

安装过程的部份图示如下：





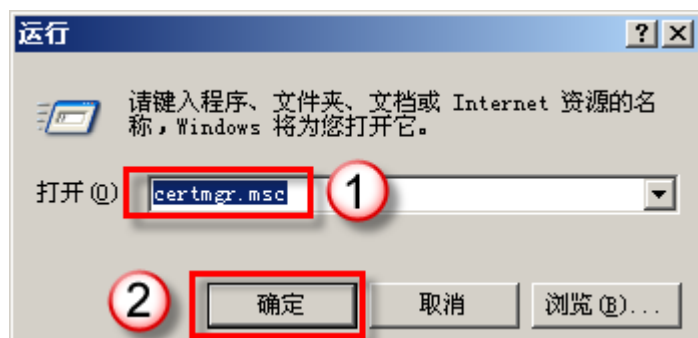
安装后，CNNIC ROOT 和 Entrust.net Secure Server Certification Authority 位于证书管理器（下面有说明如何打开证书管理器）中的在受信任的根证书颁发机构-----证书区中；而三个 CNNIC SSL 则在中级证书颁发机构-----证书区中

如果在导入证书过程中系统出现警告提示，请选择肯定的答复是(Y)，如下图所示：



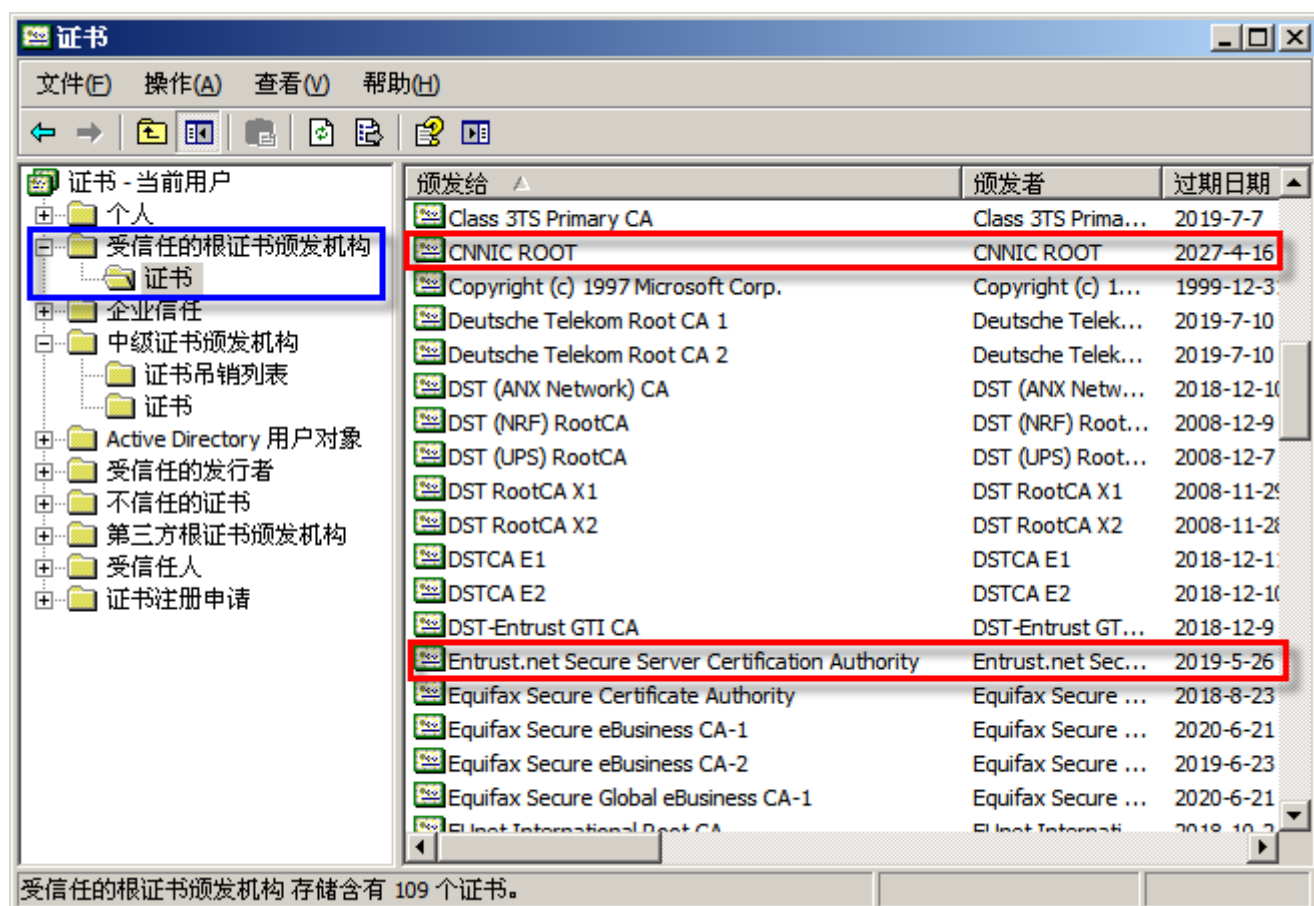
2、在证书管理器受信任的根证书颁发机构栏目中停用 CNNIC 证书

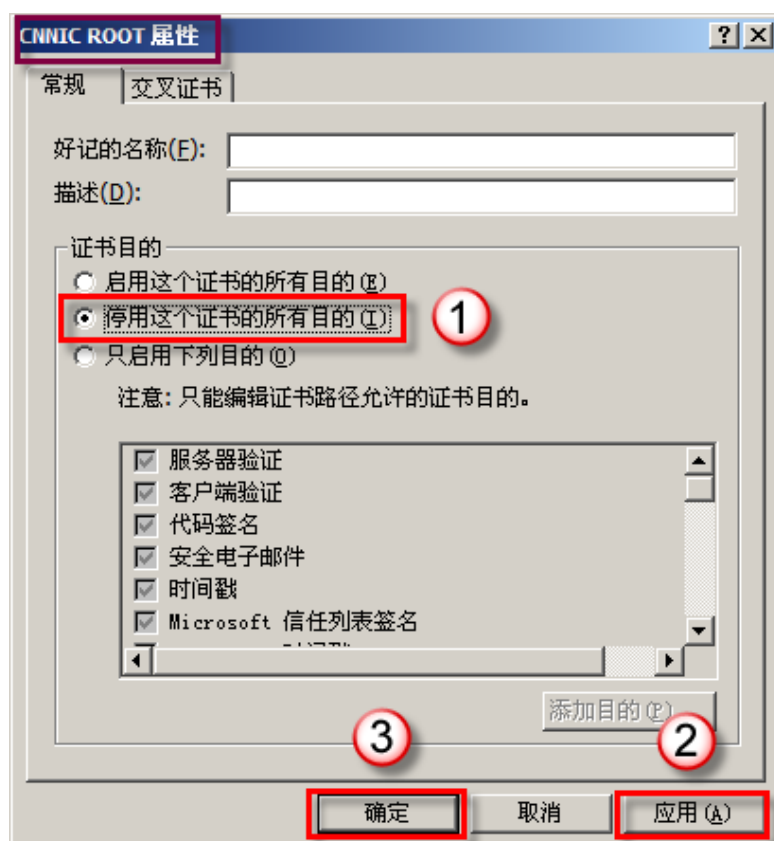
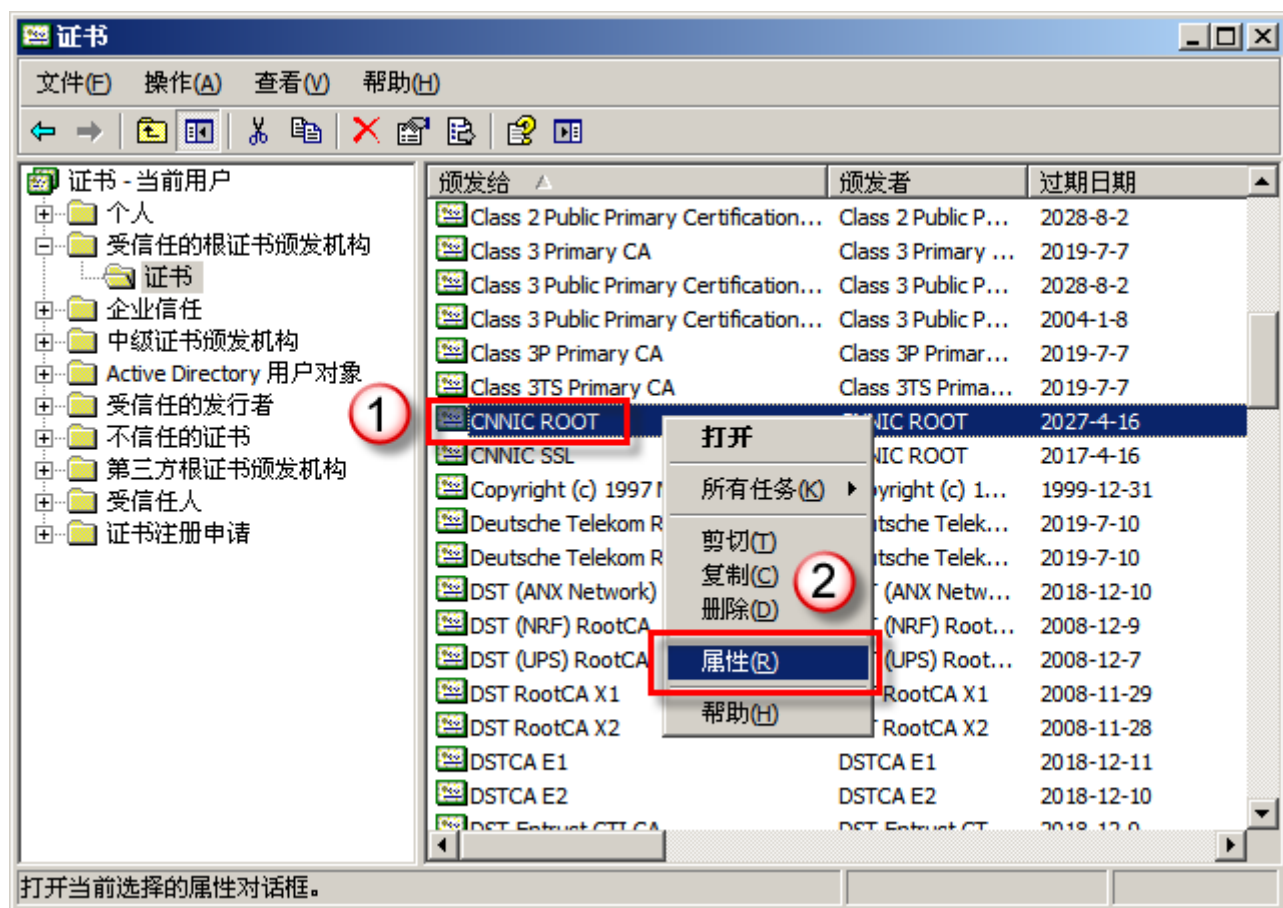
鼠标点击电脑桌面菜单 开始→运行→输入 certmgr.msc→确定，打开 Windows 的证书管理器。



停用 CNNIC ROOT 和 Entrust.netSecureServerCertificationAuthority 证书:

点击左窗口的“[受信任的根证书颁发机构](#)”前面的“+”号，再点击它的下一选项卡“[证书](#)”，可以找到两个 CNNIC 证书的位置，即：[CNNIC ROOT](#) 和 [Entrust.net Secure Server Certification Authority](#)，分别在这两项点击鼠标右键→[属性](#)→[停用这个证书的所有目的](#)→[应用](#)→[确定](#)；如果发生错误，请选择“[请继续运行并忽略此管理单元以后发生的错误](#)”。停用此 CNNIC 证书，目的是防止在线更新。

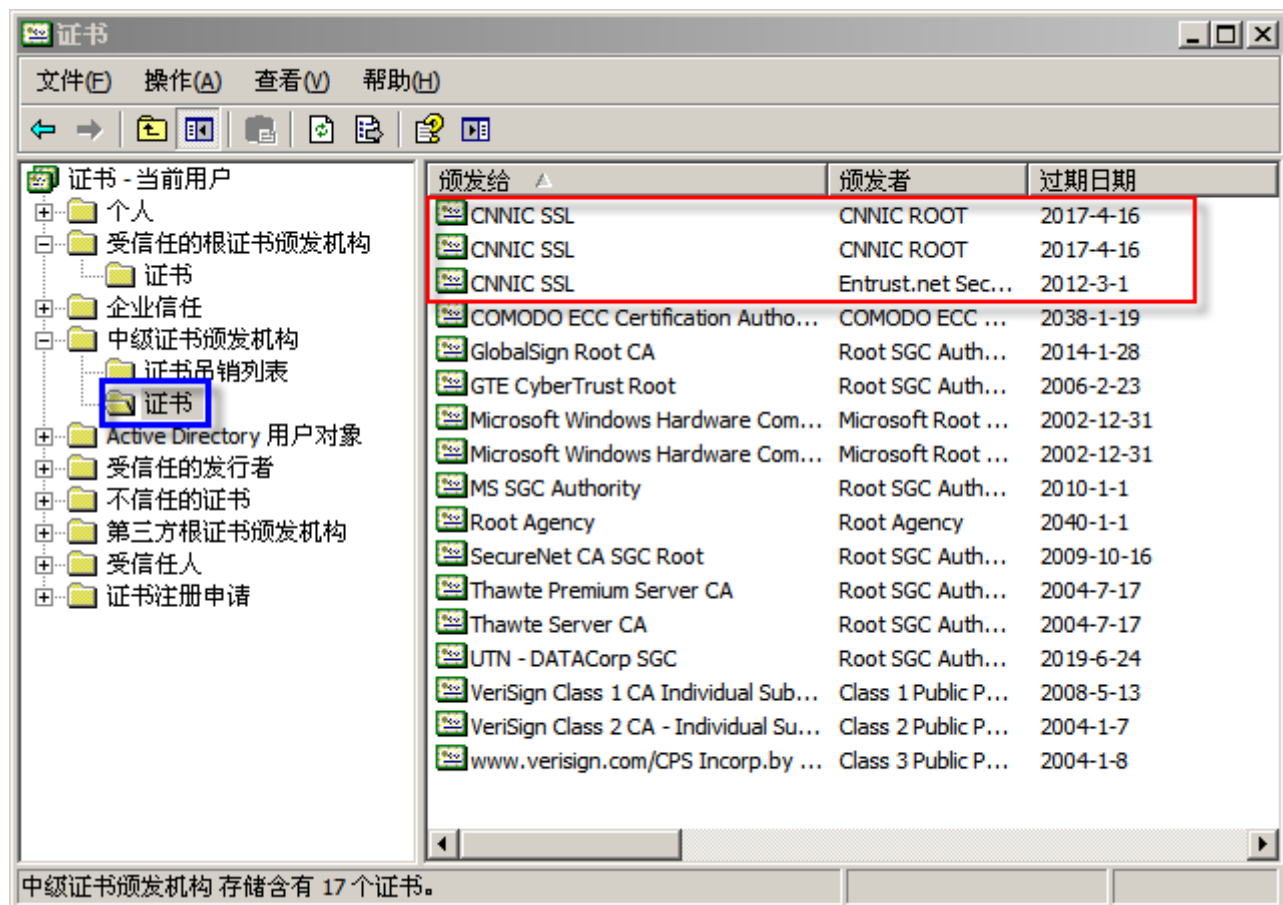




停用三个 CNNIC SSL 证书:

同上方法, 点击左窗口的“**中级证书颁发机构**”前面的“+”号, 再点击它的下一选项卡“**证书**”, 找到右面窗口下的三项 **CNNIC SSL** 内容, 分别在这三项点击鼠标右键→**属性**→**停用这个证书的所有目的**→

应用→确定；如果发生错误，请选择“请继续运行并忽略此管理单元以后发生的错误”。停用此三项 CNNIC SSL 证书，目地也是防止在线更新。



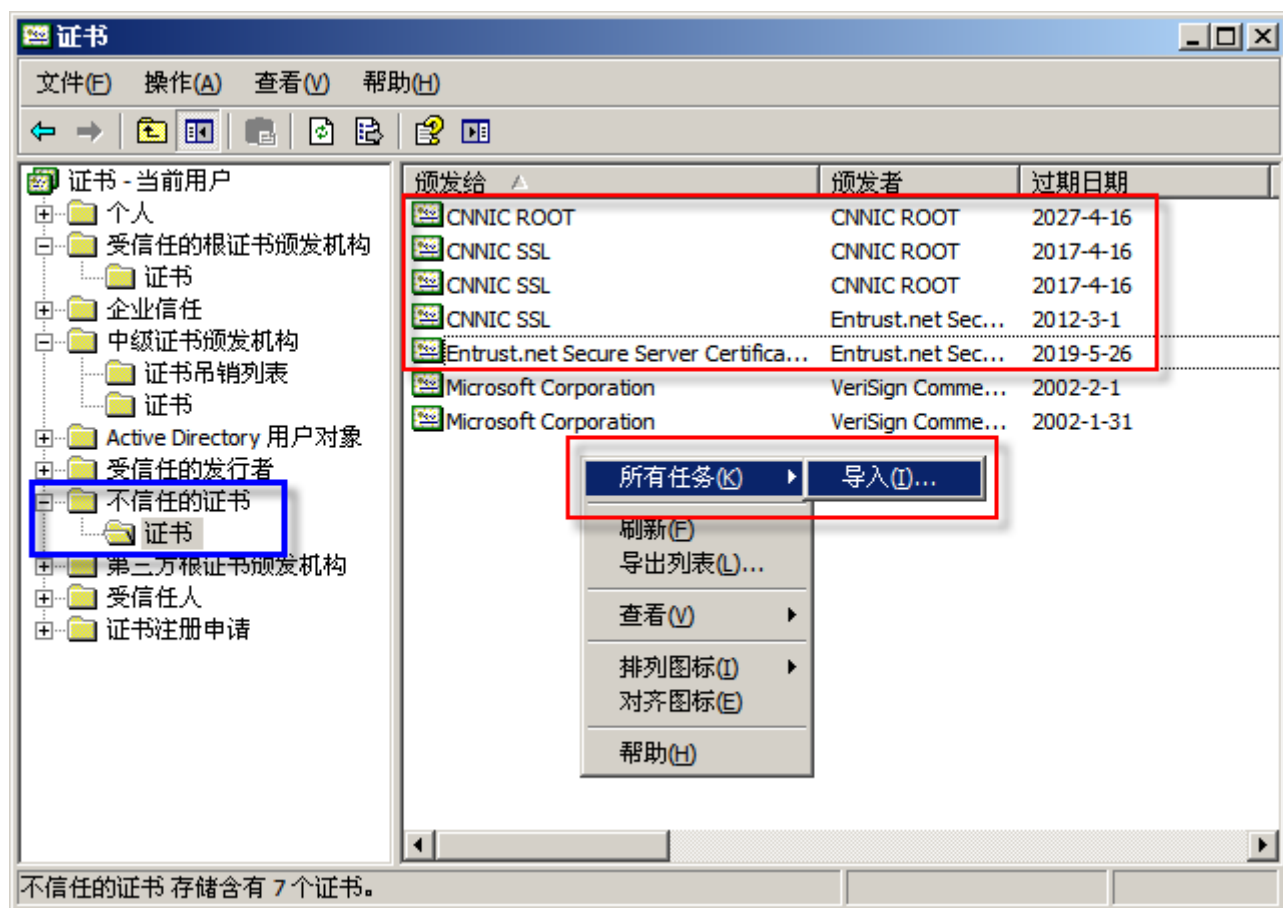
3、再次导入 CNNIC 证书并到证书管理器中的不信任的证书区域

将五个 CNNIC 证书文件再导入到不信任的证书__证书栏目里：

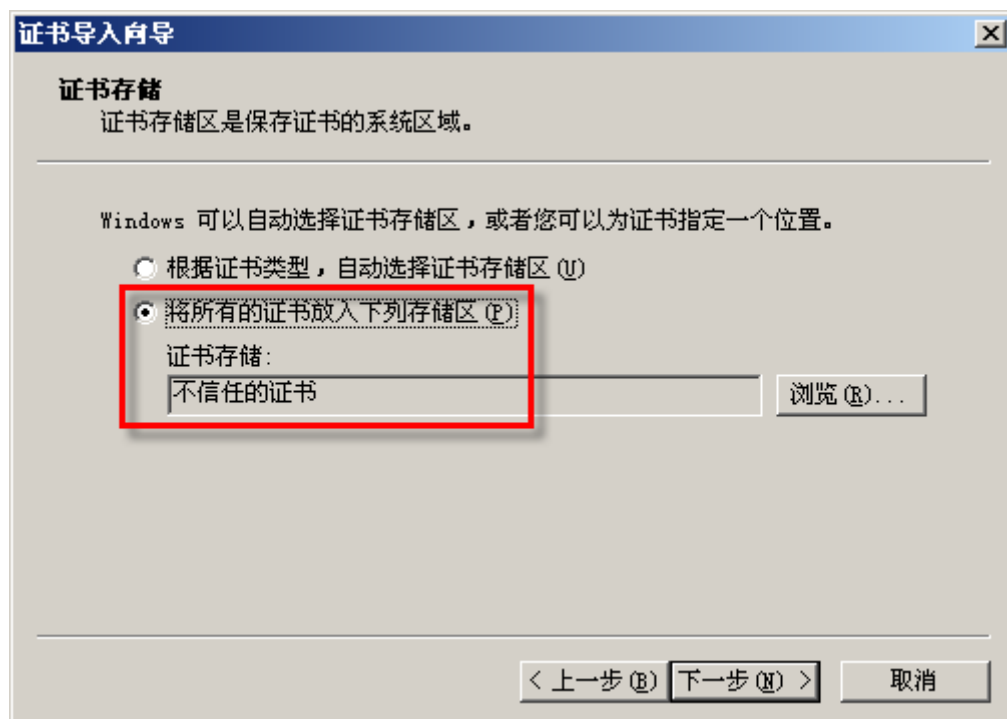
方法：打开左面的不信任的证书__证书

在右面的窗口里，点击鼠标右键→所有任务→导入→下一步→浏览→分别选取下载的五個证书文件→打开→下一步→选中“将所有的证书放入下列存储区”→下一步→完成→确定。

这样依次导入五个证书文件，如下图示：



要注意的是，前面步骤是导入到信任的证书区，这次是导入到**不信任的证书**区，以下是过程图示：



(其它步骤图示略，按上面文字说明自己完成)

4、特别说明

①对于微软的 CA 目录的证书修改，大家容易产生歧义。或许要问到为什么要先导入到信任区域，其实这个过程是配合第二步停用此证书来使用的，因为如果信任区域中如果没有 CNNIC 证书，那么在网络活动中，在访问加密站点时，系统或浏览器有可能会自动更新证书，使 CNNIC 证书被自动的加入到系统或浏览器中，并激活。如果在信任区域中有此证书但是处于停用状态，系统或浏览器就不会自动更新，

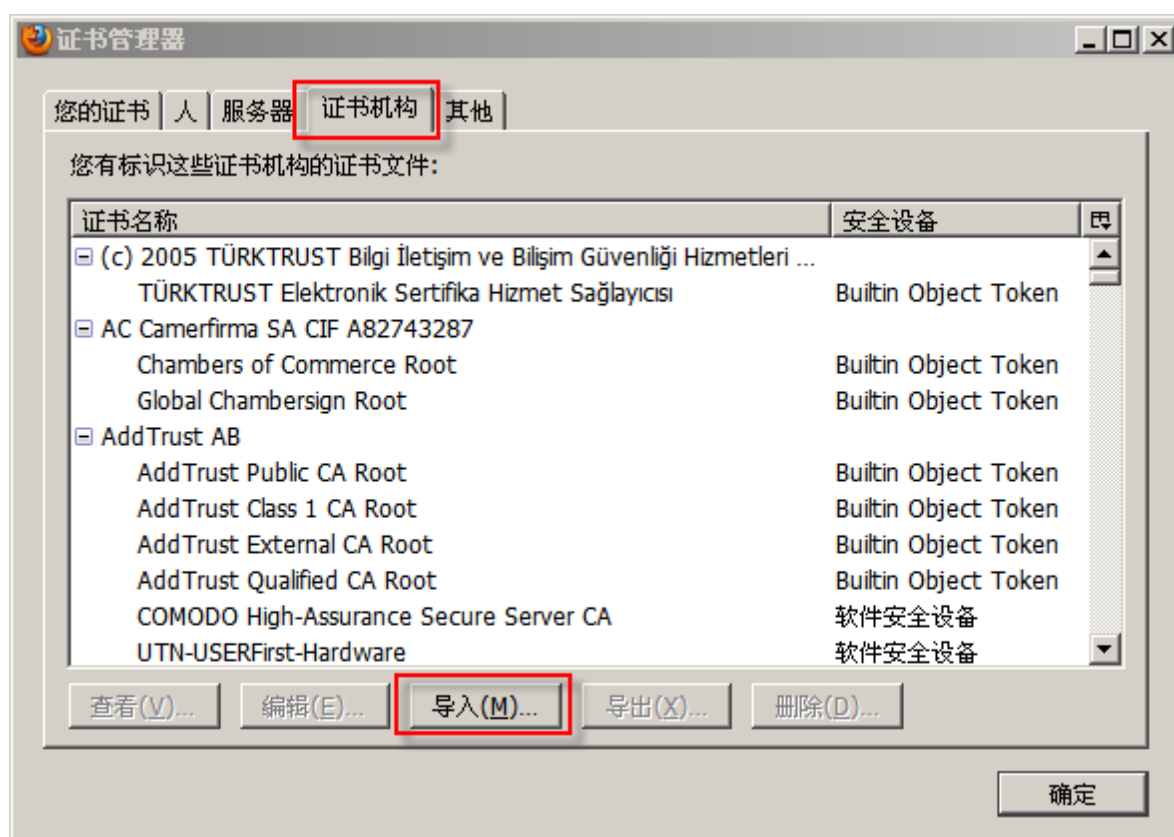
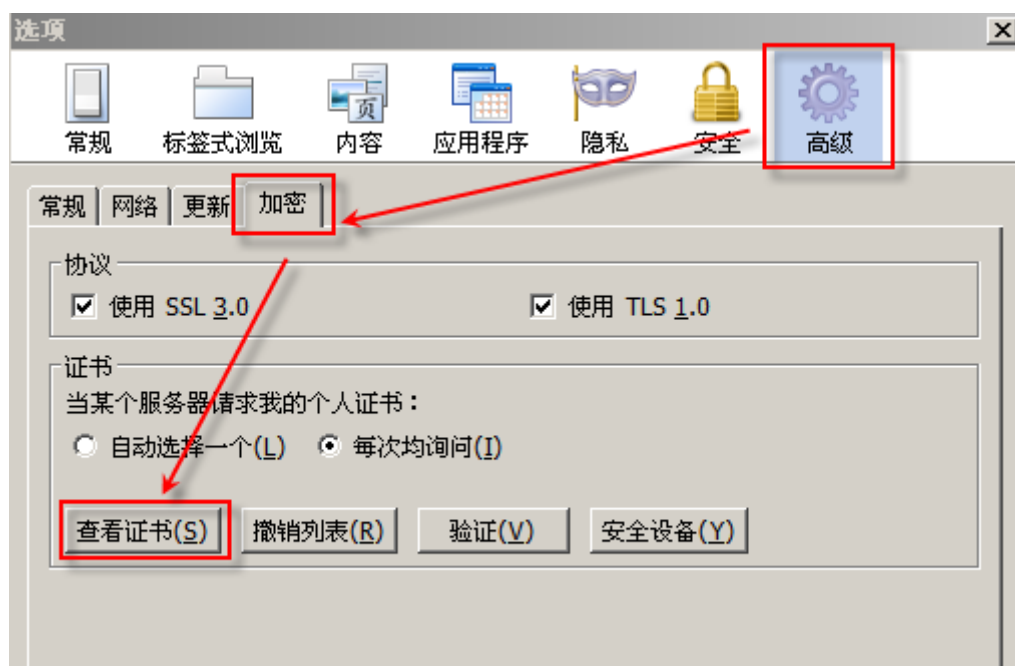
系统或浏览器会知道您是不信任此证书的。

②此方法适用于采用微软 CA 目录的浏览器，如：IE、Chrome、Safari、Dragon、Myie 等浏览器。

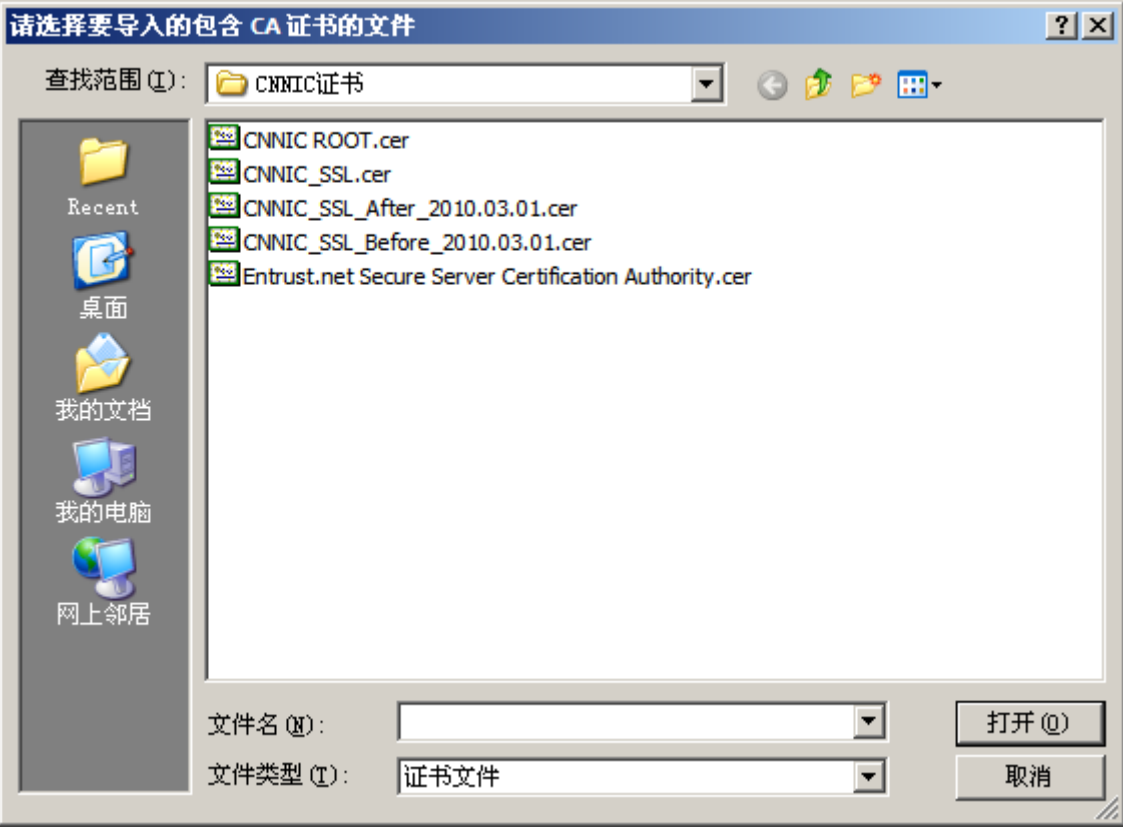
三、如何停用 Firefox 3.6 中的 CNNIC 证书

1、导入证书

打开 Firefox (或 FirefoxPortable)，点击 **工具**→**选项**→**高级**→**加密**→**查看证书(S)**→**证书机构**→**导入(M)**，如下图所示：

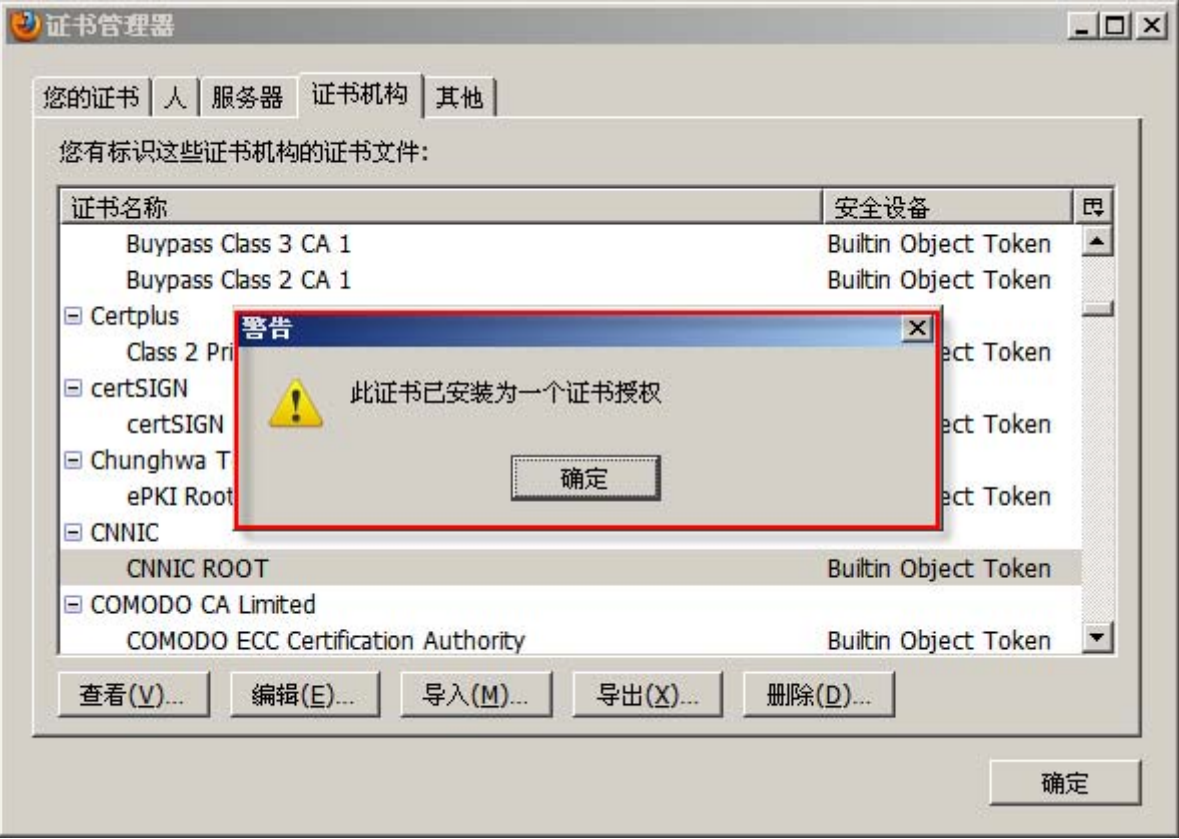


同样操作依次选中下载的五個證書文件（每次选中一个）：



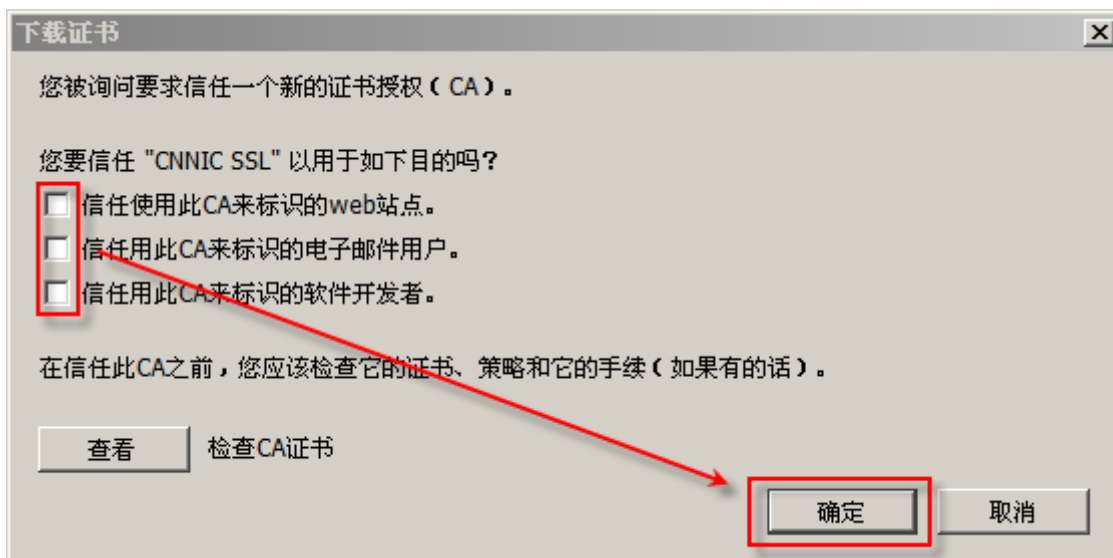
双击选择一个证书即可导入（或点击一个文件，然后点击“**打开**”）。此时会出现两种情况：

- 如果被导入的证书文件在 Firefox（或 FirefoxPortable）浏览器中已经存在，那么会看到如下图示：



这时点击按钮**确定**关闭该窗口，然后再点击**导入(M)** 按钮，继续导入后面的证书；

- 如果被导入的证书在 Firefox（或 FirefoxPortable）浏览器中不存在，就会看到如图所示情况：



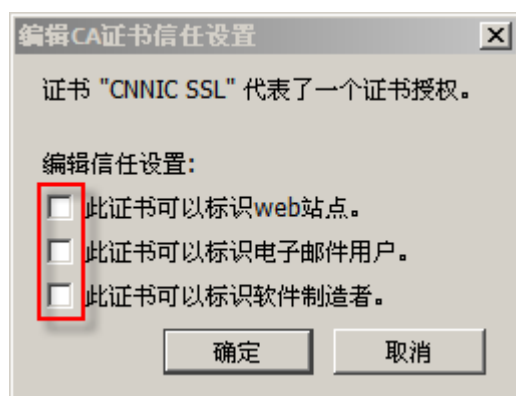
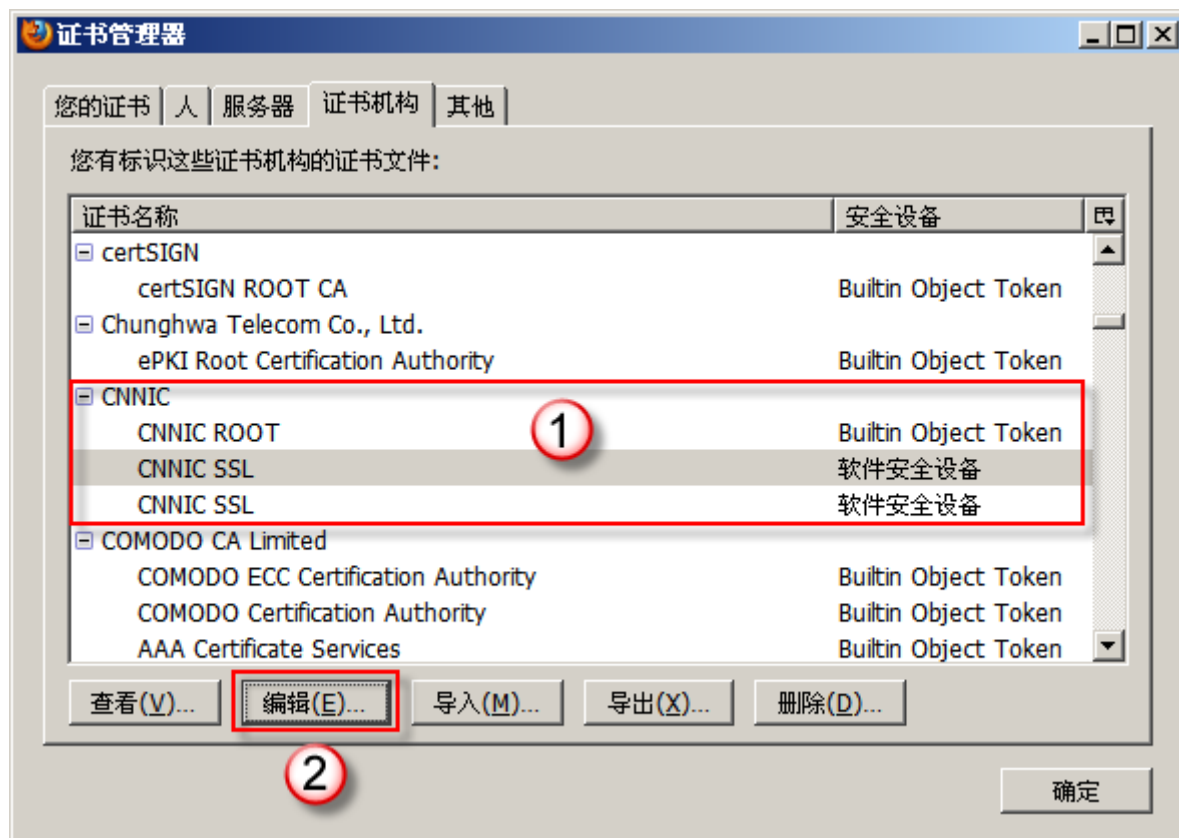
这里一般默认选项的信任设置是处于未选中状态，这时直接点击**确定**按钮即可；如果**选项**是选中状态则要先取消选中再点击**确定**按钮，窗口关闭后再点击**导入(M)** 按钮，继续导入其它的证书。

按以上步骤，将五个证书全部导入。

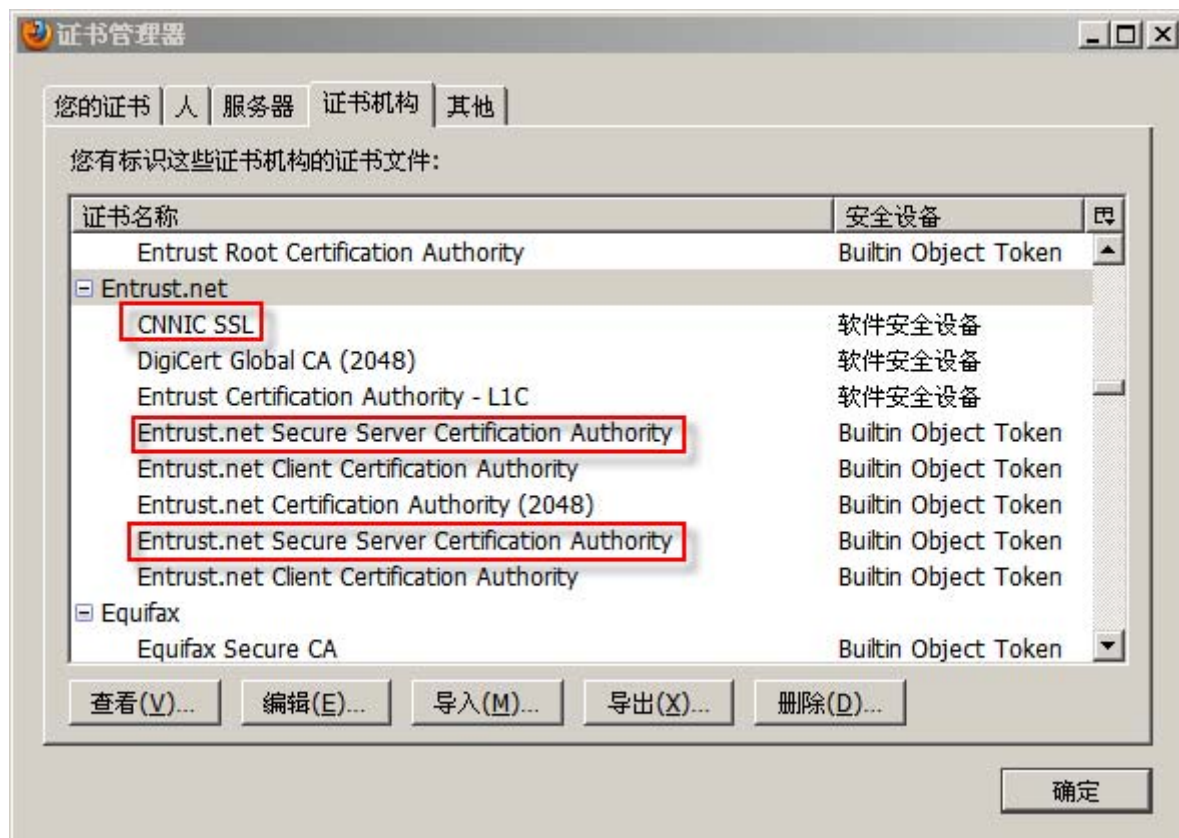
2、禁用证书

以上证书全部导入后， CNNIC 的五个证书位于不同的根级证书下，即分别位于 CNNIC 根级及 Entrust.net 根级下。

打开 Firefox（或 FirefoxPortable），点击**工具→选项→高级→加密→查看证书→证书机构**，依次找到位于 CNNIC 根级下的 **CNNIC ROOT** 和两个 **CNNIC SSL** 项，点击**编辑(E)**按钮后，取消编辑信任设置里的三个复选框**选项**即可；如果三个复选框已处于未选取状态，则直接点**确定**，如图所示：



然后再找到位于 Entrust.net 根级的 CNNIC SSL 和 Entrust.net Secure Server Certification Authority 项，按上述方法禁用。注意 Entrust.net Secure Server Certification Authority 可能有两个，我们只须禁用序列号为 **37:4A:D2:43** 的证书即可。查看序列号的方法是选中此项目后，点击“**查看(V)**”，如图所示：

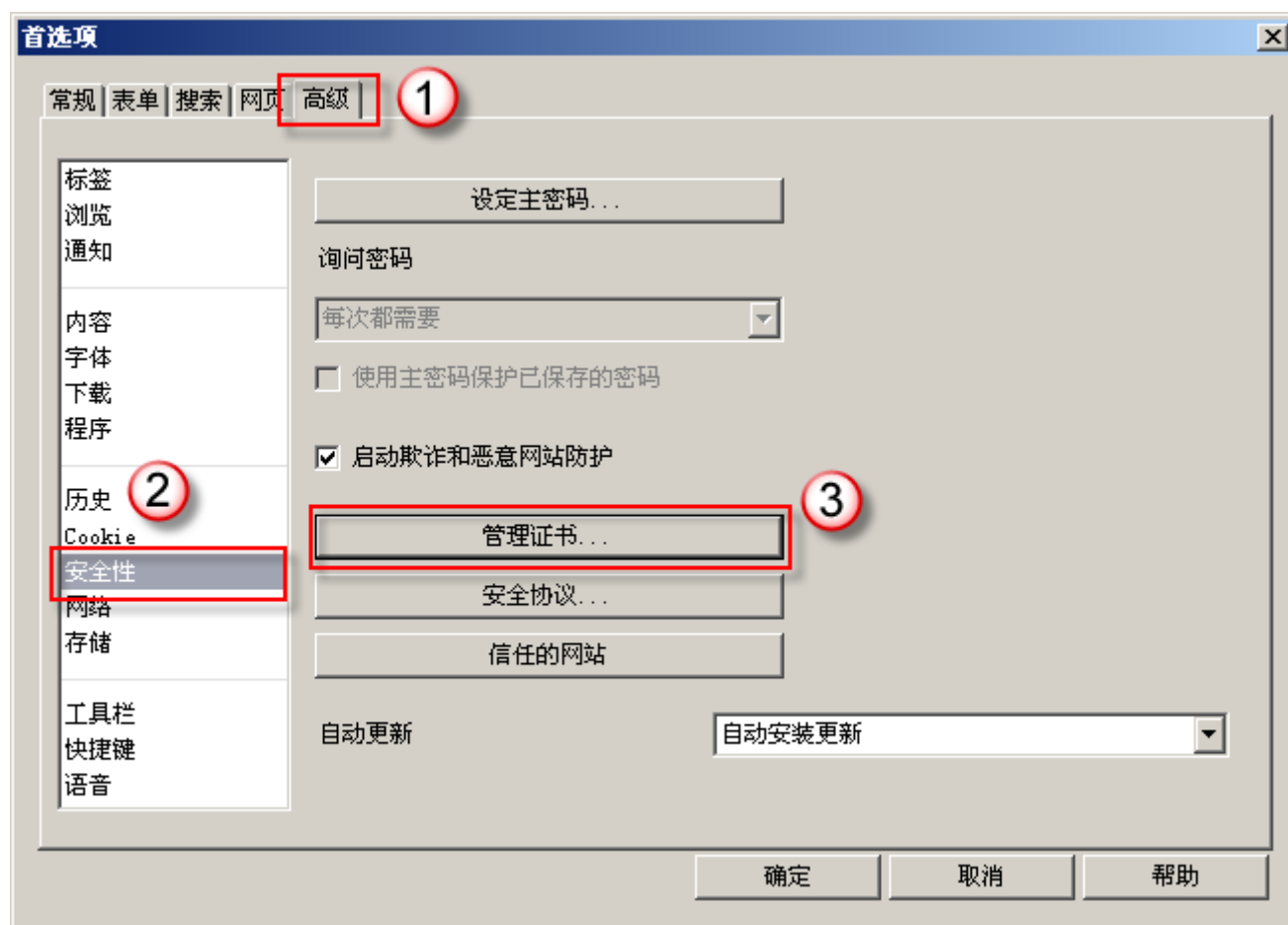


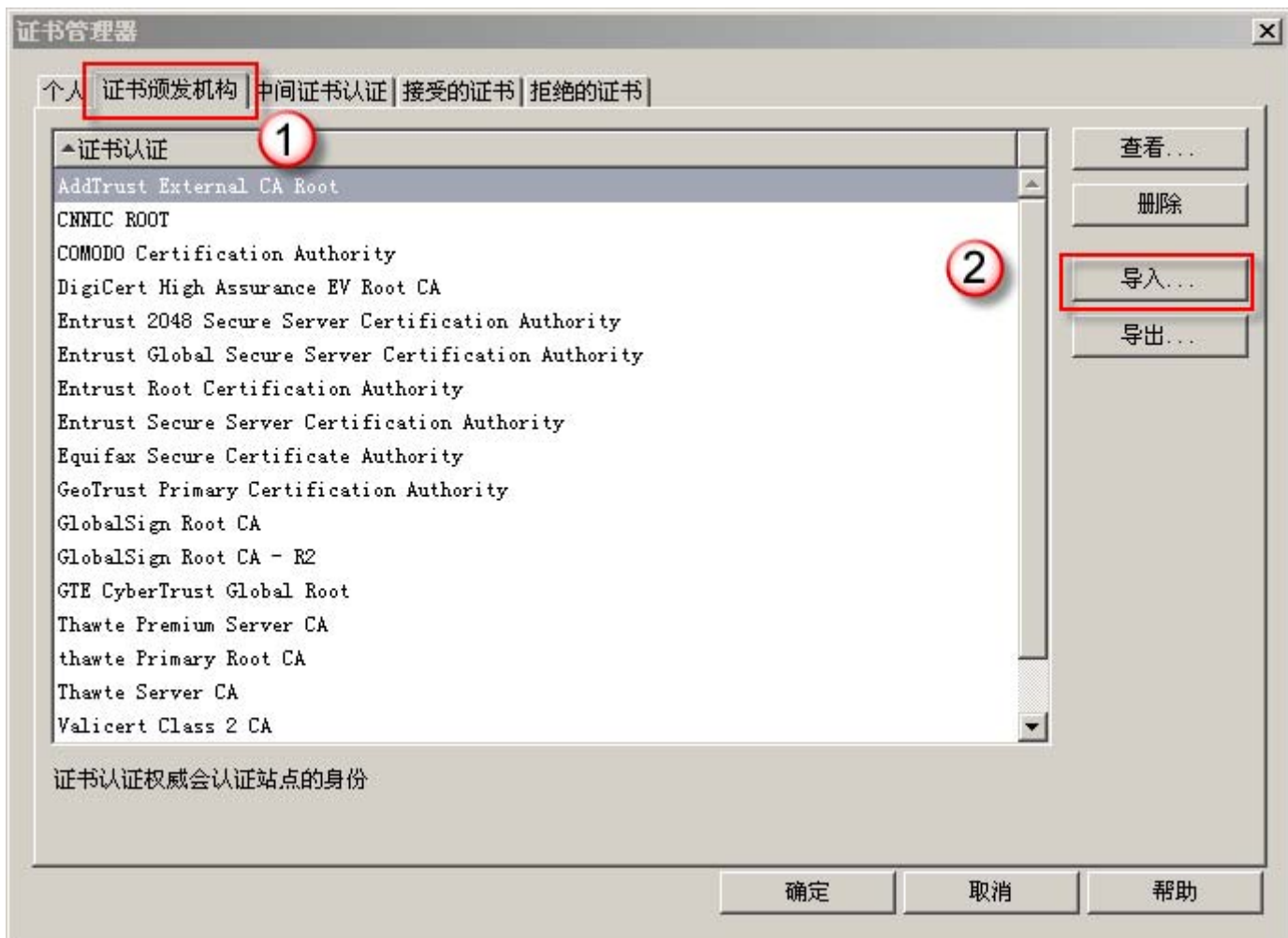
3、特别说明(必读)

Firefox（或 FirefoxPortable）默认可能没有 CNNIC 全部证书，为避免其访问加密站点时自动添加安装进来，都应按第一步导入一遍。

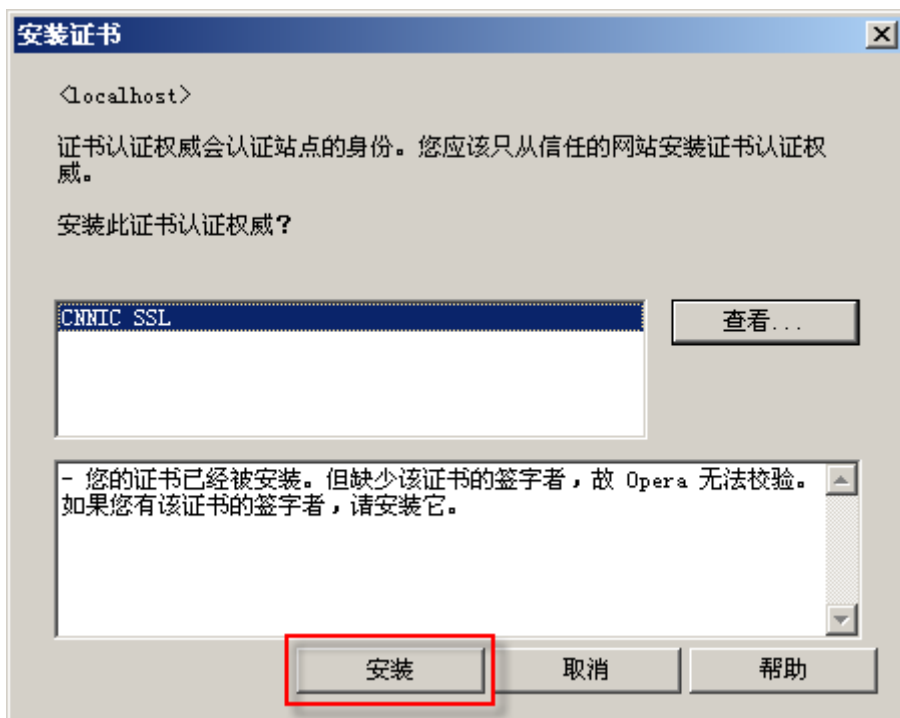
四、如何在 Opera 浏览器中停用 CNNIC 证书

以 Opera11.01 版本为例。在 Opera 浏览器中也需事先导入此五个证书。方法是启动 Opera 浏览器后，点工具→首选项→高级→安全性→管理证书→证书颁发机构→导入，如图所示：

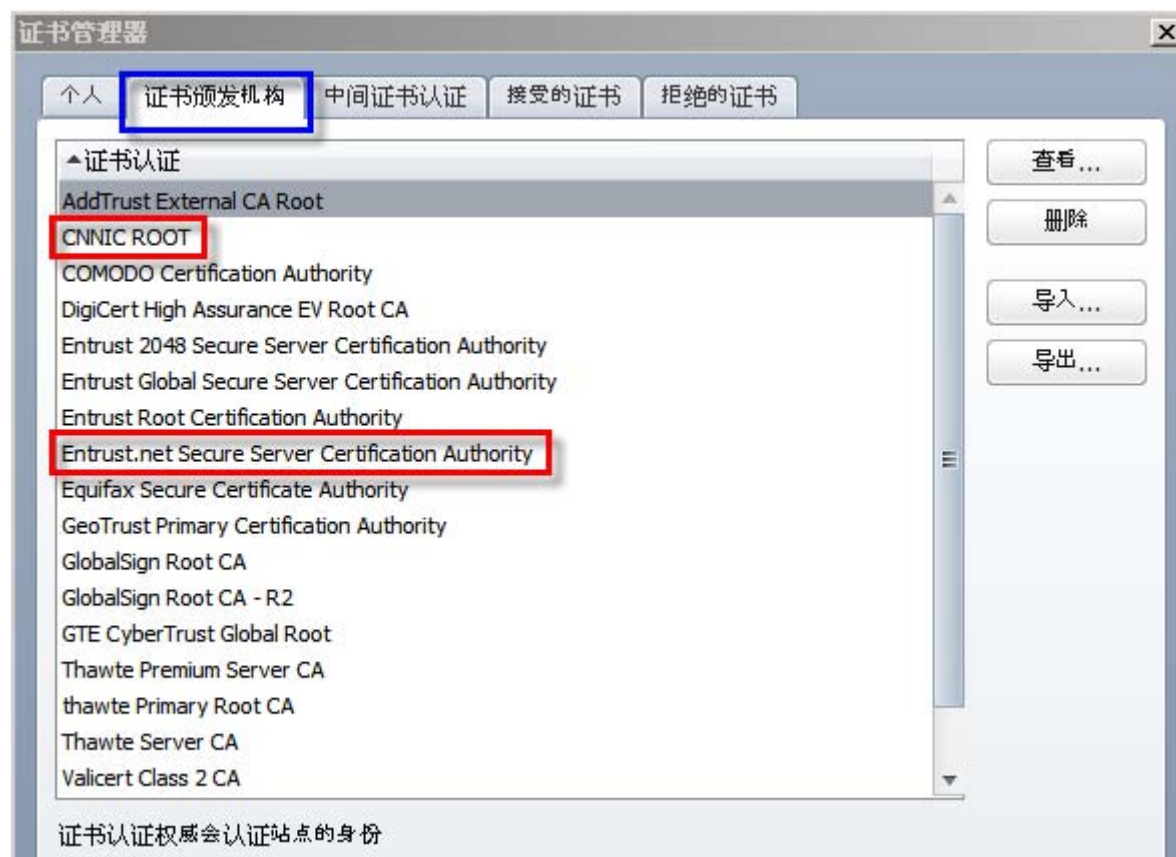




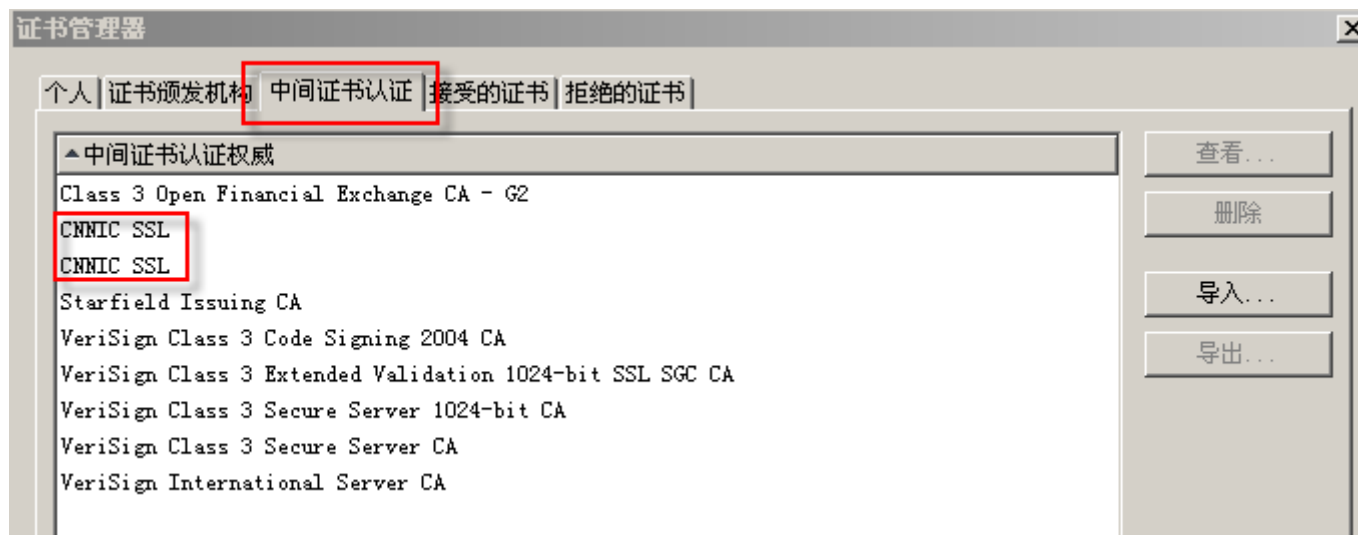
分别选取五个 CNNIC 证书，导入。在导入过程中，请选择按钮“[安装](#)”如图所示：



在 Opera 浏览器中安装后, **CNNIC ROOT** 和 **Entrust.net Secure Server Certification Authority** 位于证书管理器中的在**证书颁发机构**选项卡中, 而 **CNNIC SSL** 则在**中间证书认证**选项卡中, 如下图示:



CNNIC SSL 的位置如图所示:



特别说明

由于未知原因, 新版 Opera 11.01 没有承认序列号为 49 33 00 29 的证书, 所以上图只能列出两个 CNNIC SSL 证书, 估计是漏掉了或是 Opera 本身的 BUG, 或是别的原因。不过, 在后续的更新版本中不好确定是否有此证书, 所以请大家注意 Opera 在更新后是否有此证书。

下面我们开始在 Opera 中停用此证书:

注意: 其证书只可停用不可删除, 如果删除, 联网时它会自动更新并激活。

依次点击工具→首选项→高级→安全性→管理证书→证书颁发机构（或中间证书认证）→分别双击五个证书→取消“允许连接到使用此证书的网站”选项→确定。如下图示：



对 CNNIC SSL 和 Entrust.net Secure Server Certification Authority 证书都须进行如上处理，设置好后要从新启动 Opera 浏览器。

五、屏蔽 Mac 的 Safari 浏览器 CNNIC 证书

CNNIC 也存在于 Mac 的系统根证书中,我们可以把它设置为“不信任”。那么当你用 Safari 打开使用 CNNIC 签发的 CA 证书的网站时，同样会有提示。

具体方法如下：

- 1、打开“钥匙串”，并且在左侧面板找到“系统根证书”，然后在右侧面板找到“CNNIC”；
- 2、双击查看证书，在最上面有“信任”项目，点左边的三角将其打开，然后设置为“永不信任”；
- 3、输入用户名和密码后确定。这样，将 CNNIC 证书设为永不信任了。

六、关于部份银行网站使用 CNNIC 签名问题

国内的一些银行网站是使用了 CNNIC 证书的（不建议在破网的系统里使用网上银行）。如果主要浏览器停用 CNNIC 证书后，访问这些网上银行可换用其它没有停用 CNNIC 证书的浏览器浏览。

七、关于停用 CNNIC 证书的相关操作的重要说明（必读）

1、关于 CNNIC 五个相关证书名称的问题

CNNIC 证书共有五个，分别是：

CNNIC Root.cer （序列号 49 33 00 01）

CNNIC_SSL.cer （序列号 49 33 00 15）

CNNIC_SSL_After_2010.03.01.cer （序列号 42 87 a2 a0）

CNNIC_SSL_Before_2010.03.01.cer （序列号 49 33 00 29）

Entrust.net Secure Server Certification Authority.cer （序列号 37 4a d2 43）

系统里停用这五个证书后，在证书管理器（在桌面“开始”→“运行”里用“certmgr.msc”打开）中显示虽然的是三个“CNNIC SSL”相同字样的证书，其实这三个证书是不一样的，可以通过查看其序列号来看它们的不同。三个 CNNIC SSL 证书序列号分别为：①[49 33 00 15](#) ②[49 33 00 29](#) ③[42 87 a2 a0](#)

在没有按上面方法安装与停用这五个证书前，一般系统或浏览器这五个证书并不一定会同时存在，在访问使用 CNNIC 证书的网站时，系统里没有的 CNNIC 证书在访问某些网页时可能会被其网站自动安装到系统或浏览器里，所以，建议按上面方法将 CNNIC 五个证书全部采用先导入再禁用的步骤处理，这样可防止系统或浏览器在线更新时自动安装 CNNIC 证书到系统或浏览器里。

2、关于系统与浏览器在线更新后 CNNIC 证书停用状态是否会改变的问题

请注意，所有停用 CNNIC 证书的系统与浏览器，建议继续保持其在线更新的状态，以保证系统与浏览器处于最佳安全的状态，系统与浏览器在线自动更新并不影响已停用的 CNNIC 证书，也就是说系统与浏览器更新后 CNNIC 证书的停用状态仍然有效。如果实在不放心的，可在浏览器与浏览器在线更新后，从新检查一下证书停用状态是否仍然有效。

3、关于系统不同登录用户 CNNIC 证书停用状态的问题

①证书的停用操作只对当前Windows登录帐号起作用，如果要更换Windows帐号登录系统，那就要在新的帐号下从新按前面所述方法进行CNNIC证书的导入与停用操作；

比如，用户以 AAA 账号登录系统，按上述方法停用了 CNNIC 证书，但另一用户或同一用户在同一台计算机上以 BBB 账号登录系统时，其 CNNIC 证书还是按系统与浏览器默认设置的，这时用户 BBB 还须在 BBB 帐号下按上面方法导入与停用 CNNIC 证书；

②如果是受限帐号，必须要先将受限帐号临时提升到管理员权限，按上面所述方法将 CNNIC 证书导入与停用设置完毕后再恢复成受限帐号。

八、技术支持

大家在停用 CNNIC 证书的设置与使用过程中有什么问题，请到天地行技术网站咨询

请破网访问：<https://tiandixing.org/viewtopic.php?f=15&t=53569>

[禁书网](#)提供禁书下载阅读, 禁书目录, 禁书网<http://www.bannedbook.org/>是最大最全的禁书下载基地, 中国禁书, 大陆禁书应有尽有。

禁书禁闻禁片大陆直连: <https://pipes.yahoo.com/pipes/pipe.run?id=40fbfb511221f769a51746fa91a1ff4f>